REMARKS

Claims 1-18 are pending in this application. Claims 1-18, have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,032,257 (Olarig). Claims 1-18 have been further rejected under section 102(b) as being anticipated by U.S. Patent No. 5,778,421 (Nagano). Claims 8, 13, 14, and 15 have been cancelled. Claims 1, 11, and 16 have been amended. No new matter has been added.

Independent claims 1 and 11 include features not found in the prior art of record. Specifically, independent claim 1 as amended recites:

> A method of recording data comprising the acts of:
> receiving protected content at a data processing device;
> **determining that a portable memory recording device is trustworthy based on a proprietary hardware interface** between said data processing device and said portable memory recording device; and
> using said portable memory recording device to record said protected content onto a portable memory.

Olarig purports to teach a method of theft protection for computer related hardware (Olarig, Abstract). A digital handshake between a system and the hardware is performed, and if unsuccessful, the hardware is either crippled or disabled (Id.).

Nagano purports to teach a an information processing system for a disk-like storage medium such as flexible magnetic disks or a DVD-RAM (Nagano, Abstract). The disk-like storage devices comprise disk image data, as well as several other data sections (Id.). The disk sections are related together such that the legitimacy of the image data may be verified by confirming the relationships between the data sections (Id.).

Neither Olarig nor Nagano, alone or combination, teach **determining that a portable memory recording device is trustworthy based on a proprietary hardware interface** as set forth in amended claim 1. The Examiner states that Olarig teaches a proprietary interface because "vendor specific hardware that includes an interface contains a proprietary interface" (Office Action, page 5). Applicant respectfully submits that the use of vendor specific hardware as described in Olarig does not teach a proprietary hardware interface, and would be inoperable on a system using proprietary hardware interfaces.

Olarig is directed to the problem of computer component theft (Oliarg, col. 1, ll. 24-30). Specifically, Olarig recognizes that the proliferation of plug and play and hot swapping component architectures (i.e., non-proprietary interfaces) have made component theft easy for thieves (Id., col. 1, ll. 31-34). Because plug and play devices use a standard non-proprietary interface, e.g., PCI, ISA, USB, etc., a thief is guaranteed that a device stolen from any given computer will likely be operational on other computers, thus ensuring a market for the stolen device.

Olarig solves the problem of theft by incorporating an authentication code into the computer devices (Olarig, col. 3, ll. 17-30). When the computer system powers up, it performs a handshake operation with each of the installed computer devices where a stored authentication code on the system is compared against the authentication codes of the devices (Id.). If the devices can't be authenticated, i.e., the codes don't match, then the system disables them (Id.). Thus, a thief would have no reason to steal the installed devices because they would be presumably inoperable on other computer systems, even though the devices use a standard plug and play type interface.

However, the system of Olarig makes no mention of using a proprietary hardware interface for any of the computer devices. It is precisely because the system of Olarig uses non-proprietary (standard) hardware interfaces that the use of authentication codes is necessary or desirable. For example, if proprietary hardware interfaces were used on the computer devices, there would be no need to verify authenticity codes as described in Olarig, because the computer devices would be incapable of interfacing with the computer systems at all. Authentication using the authentication codes requires at a minimum a connection (e.g., electrical, optical, etc.) between the computer system and the computer device. Using a proprietary hardware interface prevents such a connection with unauthorized devices. Thus, the system of Olarig would be inoperable using proprietary computer devices because such a system is incapable of making the necessary connection to verify the authentication codes.

Similarly, Nagano teaches the use of non-proprietary interfaces (e.g., DVD-RAMS), and does not teach **determining that a portable memory recording device is trustworthy based on a proprietary hardware interface**. It is therefore respectfully requested that the Examiner withdraw the rejections and allow claim 1.

Claim 11 as amended contains similar (although not identical) features as claim 1, and is therefore allowable for at least the reasons given above with respect to claim 1. It is therefore respectfully requested that the Examiner withdraw the rejections and allow claim 11.

Dependent claims 2-7, 9, 10, 12, and 16-18 are all variously dependent on independent claims 1 and 11, and are therefore allowable for at least the reasons given above for the independent claims. It is therefore respectfully requested that the Examiner withdraw the rejection and allow claims 2-7, 9, 10, 12, and 16-18.

CONCLUSION

For the reasons set forth above, claims 1-7, 9-12, and 16-18 have been shown to be patentable over the applied prior art. Applicant submits that the case is in condition for allowance, and requests favorable action on the merits.

Date: July 8, 2005

Peter M. Ullman
Registration No. 43,963

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439